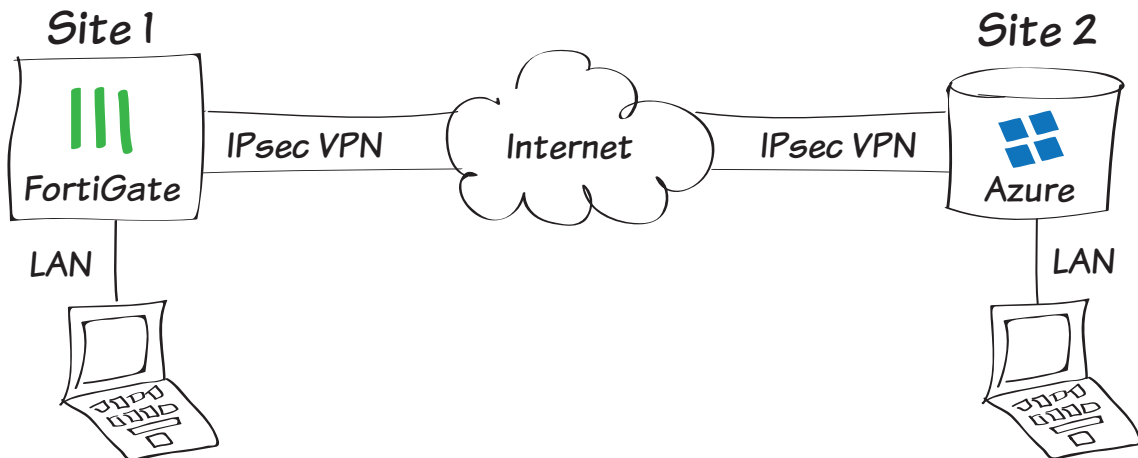


Configuring IPsec VPN between a FortiGate and Microsoft Azure™

The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is hosted on Microsoft Azure™, for which you will need a valid Microsoft Azure profile.

Using FortiOS 5.2, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied.

1. Configuring the Microsoft Azure™ virtual network
2. Creating the Microsoft Azure™ virtual network gateway
3. Configuring the FortiGate tunnel
4. Creating the FortiGate firewall addresses
5. Creating the FortiGate firewall policies
6. Results

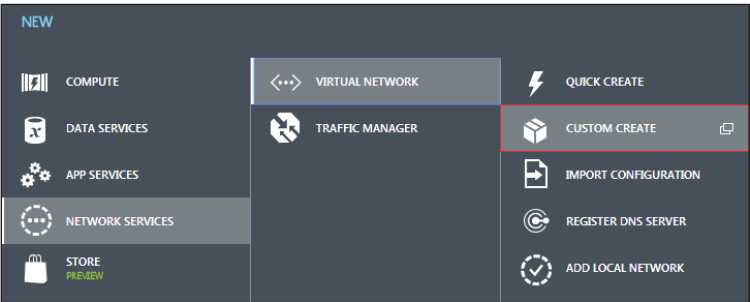


1. Configuring the Microsoft Azure™ virtual network

Log into Microsoft Azure and click **New** in the lower-left corner to add a new service.



From the prompt, select **Network Services > Virtual Network > Custom Create**.



Under ‘Virtual Network Details’, enter a **Name** for the VPN and a **Location** where you want the VMs to reside, then click the **Next** arrow.

NAME	LOCATION
Site2SiteVPN	East US

Under ‘DNS Servers and VPN Connectivity’, enable the **Configure a site-to-site VPN** checkbox and enter DNS server information if required.

Click the **Next** arrow.

DNS SERVERS ?

ENTER NAME

IP ADDRESS

POINT-TO-SITE CONNECTIVITY ?

☐ Configure a point-to-site VPN

SITE-TO-SITE CONNECTIVITY ?

☒ Configure a site-to-site VPN

☐ Use ExpressRoute

Under ‘Site-to-Site Connectivity’, enter a **Name** and **IP Address** for the FortiGate device.

Under Address Space, include a **Starting IP** and **CIDR (Address Count)** for the tunnel, avoiding overlapping subnets.

Click the **Next** arrow.

NAME	ADDRESS SPACE			
Local_Network ?	ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
VPN DEVICE IP ADDRESS ?	192.168.111.0/24	192.168.111.0	/24 (256)	192.168.111.0 - 192.168.111.255
	add address space			

Under ‘Virtual Network Address Spaces’, configure the desired address space or accept the default settings.

Select **add gateway subnet** to configure a gateway IP and click the **Checkmark** in the lower-right corner to accept the configuration.

After accepting the configuration, you will have to wait a short period of time for the virtual network to be created, but it shouldn’t be long.

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/8	10.0.0.0	/8 (16777...	10.0.0.4 - 10.255.255.254
SUBNETS			
Subnet-1	10.11.12.0	/24 (251)	10.11.12.4 - 10.11.12.254
Gateway	10.11.13.0	/29 (3)	10.11.13.4 - 10.11.13.6
add subnet		add gateway subnet	

1 OPERATION IS CURRENTLY RUNNING

Creating virtual network 'Site2SiteVPN'...

2. Creating the Microsoft Azure™ virtual network gateway

On the ‘networks’ home screen, click the name of the virtual network you just created.

NAME	STATUS
Site2SiteVPN	→ ✓ Created

Under this virtual network, go to the **Dashboard**. You will notice that the gateway has not yet been created. You will create the gateway in this step.

Site2SiteVPN

THE GATEWAY WAS NOT CREATED.

GATEWAY

VPN

Local Network

At the bottom of the screen, select **Create Gateway > Dynamic Routing**.

When prompted, select **Yes**.

Static Routing

Dynamic Routing

+

CREATE GATEWAY

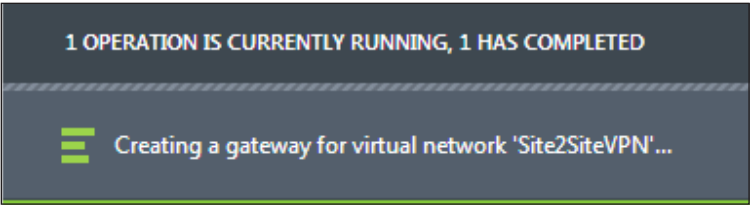
↓

EXPORT

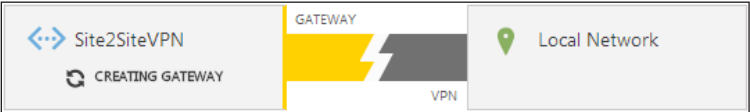
🗑

DELETE

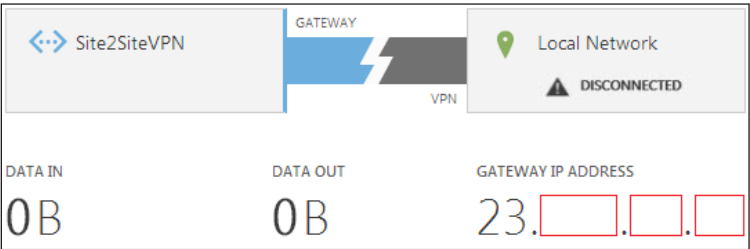
The operation to create the virtual network gateway will run. The process takes a short amount of time.



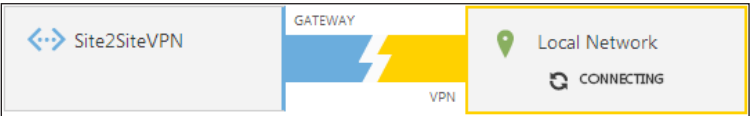
Azure will indicate to you that the gateway is being created. You may wish to leave this running for a few minutes as wait periods in excess of 10 minutes are common.



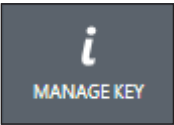
When the operation is complete, the status changes and you are given a **Gateway IP Address**.



The gateway will then attempt to connect to the Local Network.

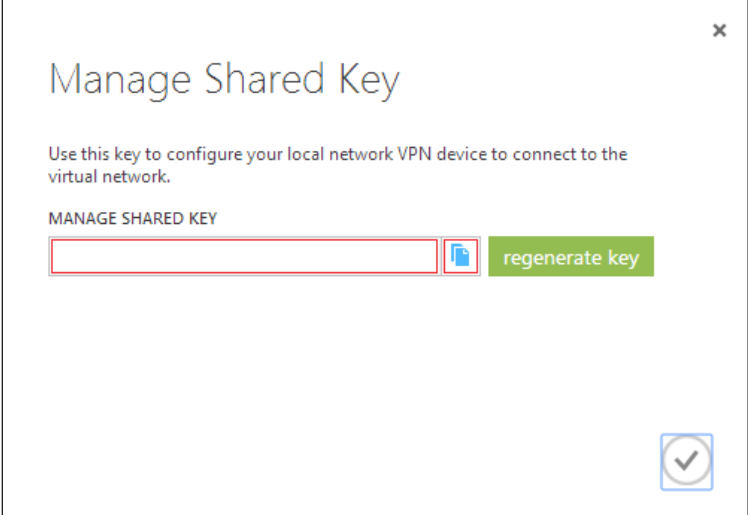


At the bottom of the screen, select **Manage Key**.



The 'Manage Shared Key' dialogue appears. **Copy** the key that is shown. You can select **regenerate key** if you want to copy a different key.

Click the **Checkmark** when you are confident that the key is copied.



The 'Manage Shared Key' dialog box has a title bar with a close button (X). The main text reads: 'Use this key to configure your local network VPN device to connect to the virtual network.' Below this is a section titled 'MANAGE SHARED KEY' containing a text input field with a red border, a copy icon, and a green 'regenerate key' button. In the bottom right corner, there is a blue square button with a white checkmark.

You are now ready to configure the FortiGate endpoint of the tunnel.

3. Configuring the FortiGate tunnel

Go to **VPN > IPsec > Wizard** and select **Custom VPN Tunnel (No Template)**.

Enter a **Name** for the tunnel and click **Next**.



The 'VPN Setup' wizard is shown with a blue header bar containing a '1' and the text 'VPN Setup'. The 'Name' field contains 'Site2Site'. Under the 'Template' section, a list of options is shown: 'Dialup - FortiClient (Windows, Mac OS, Android)', 'Site to Site - FortiGate', 'Dialup - iOS (Native)', 'Dialup - Android (Native L2TP/IPsec)', 'Dialup - Cisco Firewall', 'Site to Site - Cisco', and 'Custom VPN Tunnel (No Template)'. The last option is selected and highlighted in blue. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter the desired parameters. Set the **Remote Gateway** to **Static IP Address**, and include the gateway **IP Address** provided by Microsoft Azure.

Set the **Local Interface** to **wan1**.

Under **Authentication**, enter the **Pre-shared Key** provided by Microsoft Azure.

Disable **NAT Traversal** and **Dead Peer Detection**.

Name

Site2Site

Comments

Comments

Enable IPsec Interface Mode

☒

Network

IP Version

☒ IPv4

☐ IPv6

Remote Gateway

Static IP Address

IP Address

Local Interface

wan1

Mode Config

☐

NAT Traversal

☐

Dead Peer Detection

☐

Under **Authentication**, ensure that you enable **IKEv2** and set **DH Group** to **2**.

Enable the encryption types shown and set the **Keylife** to **56600** seconds.

Authentication

Method

Pre-shared Key

Pre-shared Key

.....

Show Key

IKE

Version

☐ 1

☒ 2

Phase 1 Proposal

Encryption

AES256

Authentication

SHA1

Remove

Encryption

AES256

Authentication

SHA256

Remove

Encryption

AES128

Authentication

SHA1

Remove

Encryption

AES128

Authentication

SHA256

Remove

Diffie-Hellman Group

☐ 21

☐ 20

☐ 19

☐ 18

☐ 17

☐ 16

☐ 15

☐ 14

☐ 5

☒ 2

☐ 1

Key Lifetime (seconds)

56600

Local ID

Scroll down to **Phase 2 Selectors** and set **Local Address** to the local subnet and **Remote Address** to the VPN tunnel endpoint subnet (found under 'Virtual Network Address Spaces' in Microsoft Azure).

Enable the encryption types to match Phase 1 and set the **Keylife** to **7200** seconds.

The screenshot shows the 'Phase 2 Selectors' configuration page. At the top, a table lists the selectors: 'Site2Site' with 'Local Address' '192.168.111.0/255.255.255.0' and 'Remote Address' '10.11.12.0/255.255.255.0'. Below this is the 'Edit Phase 2' section for 'Site2Site', showing its comments and the same address ranges. The 'Advanced...' section contains the 'Phase 2 Proposal' settings: four encryption/authentication pairs (AES128/SHA256, AES256/SHA256, AES128/SHA1, AES256/SHA1), 'Enable Replay Detection' checked, 'Enable Perfect Forward Secrecy (PFS)' unchecked, and port/protocol settings all set to 'All'. The 'Key Lifetime' is set to '7200' seconds.

Phase 2 Selectors		
Name	Local Address	Remote Address
Site2Site	192.168.111.0/255.255.255.0	10.11.12.0/255.255.255.0

Edit Phase 2

Name: Site2Site

Comments: VPN: Site2Site (Created by VPN wizard)

Local Address: Subnet 192.168.111.0/255.255.255.0

Remote Address: Subnet 10.11.12.0/255.255.255.0

Advanced...

Phase 2 Proposal

Encryption: AES128 Authentication: SHA256 Remove

Encryption: AES256 Authentication: SHA256 Remove

Encryption: AES128 Authentication: SHA1 Remove

Encryption: AES256 Authentication: SHA1 Remove

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☐

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Autokey Keep Alive ☐

Auto-negotiate ☐

Key Lifetime: Seconds

Seconds: 7200

4. Creating the FortiGate firewall addresses

Go to **Policy & Objects > Objects > Addresses** and configure a firewall address for the local network.

The screenshot shows the 'Address' configuration page. The 'Category' is 'Address'. The 'Name' is 'Internal_Port1'. The 'Type' is 'Subnet'. The 'Subnet / IP Range' is '192.168.111.0/255.255.255.0'. The 'Interface' is 'any'. 'Visibility' is checked. The 'Comments' field is empty. The page has 'OK' and 'Cancel' buttons at the bottom.

Category: ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name: Internal_Port1

Type: Subnet

Subnet / IP Range: 192.168.111.0/255.255.255.0

Interface: any

Visibility: ☒

Comments: Write a comment... 0/255

OK Cancel

Create another firewall object for the Azure VPN tunnel subnet.

Category

Address

IPv6 Address

Multicast Address

Name

AzureVPN-tunnel

Type

Subnet

Subnet / IP Range

10.11.12.0/255.255.255.0

Interface

any

Visibility

Comments

Write a comment...

0/255

OK

Cancel

5. Creating the FortiGate firewall policies

Go to **Policy & Objects > Policy > IPv4** and create a new policy for the site-to-site connection that allows outgoing traffic.

Set the **Source Address** and **Destination Address** using the firewall objects you just created.

Incoming Interface

internal1

Source Address

Internal_Port1

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

Site2Site

Destination Address

AzureVPN-tunnel

Schedule

always

Service

ALL

Action

ACCEPT

When you are done, create another policy for the same connection to allow incoming traffic.

This time, invert the **Source Address** and **Destination Address**.

Incoming Interface

Site2Site

Source Address

AzureVPN-tunnel

Source User(s)

Click to add...

Source Device Type

Click to add...

Outgoing Interface

internal1

Destination Address

Internal_Port1

Schedule

always

Service

ALL

Action

ACCEPT

6. Results

Go to **VPN > Monitor > IPsec Monitor**. Right-click the tunnel you created and select **Bring Up** to activate the tunnel.

Name	Type	Remote Gateway	Username	Status
Site2Site	Static IP or Dynamic DNS			Down

Name	Type	Remote Gateway	Username	Status
Site2Site	Static IP or Dynamic DNS			Up

Go to **Log & Report > Event Log > VPN**.

Select an entry to view more information and verify the connection.

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
12	15:23:04	<div><div></div></div>	phase2-up		IPsec phase 2 status change	Site2Site
13	15:23:04	<div><div></div></div>	install_sa		install IPsec SA	Site2Site
14	15:23:04	<div><div></div></div>	negotiate	success	negotiate IPsec phase 2	Site2Site
15	15:23:04	<div><div></div></div>	negotiate	success	progress IPsec phase 1	Site2Site
16	15:23:04	<div><div></div></div>	negotiate	success	negotiate IPsec phase 1	Site2Site
<div><div></div><div></div><div>1</div><div>/ 1582</div><div></div><div></div><div>[Total: 79053]</div></div>						
Action	negotiate			Assigned IP	N/A	
Cookies	9de897c069896c80/31b2351571a476b2			Date/Time	15:23:04 (1407770584)	
ESP Authentication	HMAC_SHA1			ESP Transform	ESP_AES	
Group	N/A			IPsec Local IP	69.171.153.181	
IPsec Remote IP	23.100.122.11			Level	notice <div><div></div></div>	
Local Port	500			Log Description	negotiate IPsec phase 2	
Log ID	37186			Message	negotiate IPsec phase 2	
Outgoing Interface	ppp1			Remote Port	500	
Role	initiator			Status	success	
Sub Type	vpn			Timestamp	8/11/2014, 3:23:04 PM	
User	<div><div></div></div> N/A			VPN Tunnel	Site2Site	
Virtual Domain	root			XAUTH Group	N/A	
XAUTH User	N/A					

Return to the Microsoft Azure virtual network **Dashboard**. The status of the tunnel will show as **Connected**.

Data In and **Data Out** will indicate that traffic is flowing.

